

Ruby - Bug #6143

Onigmo allows broken regexp: /(?(x.)/

03/14/2012 07:40 PM - mame (Yusuke Endoh)

Status:	Closed	Backport:
Priority:	Normal	
Assignee:	naruse (Yui NARUSE)	
Target version:		
ruby -v:	ruby 2.0.0dev (2012-03-14 trunk 35017) [i686-linux]	

Description

naruse k-takata

Onigmo

```
$ ./miniruby -e 'p /(?(x.)/'
/(?(x.)/

$ valgrind ./miniruby -e "'x'[/?(x)/]'
(
==25802== Conditional jump or move depends on uninitialised value(s)
==25802== at 0x210DE2: match_at (regex.c:2875)
==25802== by 0x214F09: onig_search_gpos (regex.c:4172)
==25802== by 0x215B02: onig_search (regex.c:3877)
==25802== by 0x1FE91A: rb_reg_search (re.c:1373)
==25802== by 0x242A98: rb_str_aref_m (string.c:3128)
==25802== by 0x287E04: call_cfunc (vm_insnhelper.c:365)
==25802== by 0x299FC6: vm_call_method (vm_insnhelper.c:452)
==25802== by 0x28CB03: vm_exec_core (insns.def:1906)
==25802== by 0x2934A9: vm_exec (vm.c:1223)
==25802== by 0x29B5CA: rb_iseq_eval_main (vm.c:1463)
==25802== by 0x1615D3: ruby_exec_internal (eval.c:204)
==25802== by 0x48EE112: (below main) (libc-start.c:226)
(
regparse.c parse_enclose
4970 case '(': /* conditional expression: (?(cond)yes), (?(cond)yes|no) */
Coverity Scan
--
Yusuke Endoh mame@tsg.ne.jp
```

History

- #1 - 03/15/2012 11:30 PM - k_takata (Ken Takata)
- Onigmo master
- <https://github.com/k-takata/Onigmo/commit/35f530676970e42b83b5d6789dd5820101e430d7>
- Onigmo
- #2 - 03/18/2012 06:46 PM - shyouhei (Shyouhei Urabe)
- Status changed from Open to Assigned
- #3 - 03/21/2012 01:42 AM - k_takata (Ken Takata)

Onigmo Ruby
<https://github.com/k-takata/Onigmo/tree/tmp/ruby-2.0.x>

#4 - 03/22/2012 09:20 AM - naruse (Yui NARUSE)
- Status changed from Assigned to Closed